wherein said verifying value is independently generated and stored in said memory device in association with a category of the contents data.

20. (New) The data processing apparatus of claim 19, wherein the device computes the verifying value based on data from the individual contents data and then compares the computed verifying value to a previously stored verifying value, and finally utilizes the individual contents data solely in the case in which both values are identified to be coincident with each other.

21. (New) The data processing apparatus of claim 19, wherein the memory device stores contents data of a variety of categories corresponding to a plurality of directories; and wherein the verifying value is generated to deal with an assemblage of contents data individually corresponding to the plurality of directories.

22. (New) The data processing apparatus of claim 19, wherein the memory device comprises a flash memory; and the verifying value associated with the category is stored in a domain preset as a utilization inhibited block in said flash memory.

23. (New) The data processing apparatus of claim 19, wherein a plurality of verifying values are independently generated and stored in the memory device in association with respective categories of contents data.

24. (New) The data processing apparatus of claim 19, wherein a plurality of categories of contents data are individually preset based on a controlling entity of an enabling

key block which enciphers a contents key functioning as a contents enciphering key and then delivers said contents key to the device; and wherein a plurality of verifying values are independently generated and stored in the memory device in association with each of the plurality of categories of contents data.

25. (New) The data processing apparatus of claim 19, wherein the verifying value is individually generated based on a message authentication code, which is generated by applying a Data Encryption Standard to a partial data message comprising data to be subject to verification via said verifying value.

26. (New) A data processing apparatus comprising:

a memory device for storing contents data; and

a device for (a) generating and storing message authentication codes functioning themselves as the data for probing an act of tampering with the stored contents data, (b) generating a plurality of message authentication codes from different data domains, wherein part of the data domains used for generating said message authentication codes therein comprise common data; and (c) renewing the common data whenever renewing any of the plural message authentication codes for use in renewing other message authentication codes.

27. (New) A method for use in a data processing apparatus, the method comprising the steps of:

initially generating a verifying value for verifying an individual contents data to be stored in a memory device;

storing the verified value in the memory device in correspondence with the contents data; and

checking to probe actual occurrence or absence of the act of tampering with said contents data by referring to said verifying value;

wherein said verifying value is independently generated and stored in said memory device in association with a category of the contents data.

28. (New) The method of claim 27, further comprising the steps of:

computing the verifying value based on data from the individual contents data; and

comparing the computed verifying value to a previously stored verifying value;

using the individual contents data solely in the case in which both values are identified to be coincident with each other.

29. (New) The method of claim 27, wherein the memory device performs the step of storing contents data of a variety of categories corresponding to a plurality of directories; and wherein the verifying value is generated to deal with an assemblage of contents data individually corresponding to the plurality of directories.

30. (New) The method of claim 27, wherein the memory device comprises a flash memory; and the verifying value associated with the category is stored in a domain preset as a utilization inhibited block in said flash memory.

31. (New) The method of claim 27, wherein a plurality of verifying values are independently generated and stored in the memory device in association with respective categories of contents data.

32. (New) The method of claim 27, wherein a plurality of categories of contents data are individually preset based on a controlling entity of an enabling key block which enciphers a contents key functioning as a contents enciphering key and then delivers said contents key to the data processing apparatus; and wherein a plurality of verifying values are independently generated and stored in the memory device in association with each of the plurality of categories of contents data.

33. (New) The method of claim 27, wherein the verifying value is individually generated based on a message authentication code, which is generated by applying a Data Encryption Standard to a partial data message comprising data to be subject to verification via said verifying value.

34. (New) The method of claim 27 further comprising the steps of:

generating a plurality of message authentication codes from different data domains, wherein part of the data domains used for generating said message authentication codes therein comprise common data; and

renewing the common data whenever renewing any of the plural message authentication codes for use in renewing other message authentication codes.

35. (New) A method for use in a data processing apparatus, the method comprising the steps of:

generating a plurality of message authentication codes from different data domains, wherein part of the data domains used for generating said message authentication codes therein comprise common data; and

renewing the common data whenever renewing any of the plural message authentication codes for use in renewing other message authentication codes.

36. (New) A computer-readable medium for storing computer-executable software code, the code comprising:

code for initially generating a verifying value for verifying an individual contents data to be stored in a memory device;

a'

code for storing the verified value in the memory device in correspondence with the contents data; and

code for checking to probe actual occurrence or absence of the act of tampering with said contents data by referring to said verifying value;

wherein said verifying value is independently generated and stored in said memory device in association with a category of the contents data.